The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/26/2014

SUBJECT:

Vulnerability found in Adobe Flash Player Could Allow Remote Code Execution (APSB14-26)

EXECUTIVE SUMMARY:

A vulnerability in Adobe Flash Player may allow remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages.

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

This vulnerability is actively being exploited in the wild by multiple exploit kits.

SYSTEM AFFECTED:

- Adobe Flash Player 15.0.0.223 and earlier versions
- Adobe Flash Player 13.0.0.252 and earlier 13.x versions
- Adobe Flash Player 11.2.202.418 and earlier versions for Linux

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Adobe Flash Player is prone to a vulnerability that could allow for remote code execution due to an error in the handling of a dereferenced memory pointer (CVE-2014-8439).

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user access.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

REFERENCES:

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-26.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8439

F-Secure:

https://www.f-secure.com/weblog/archives/00002768.html